REMARKS

Applicants appreciate the thorough examination of the present application as reflected in the Official Action mailed September 22, 2004. Applicants have amended the specification to provide the serial number of the related case and to correct a typographic error. Applicants have also amended Claim 5 to clarify that the plurality of personal keys are based on the current passphrase. Applicants submit that the present application is in condition for allowance for at least the reasons discussed below.

The Section 112 Rejection

Claims 5 and 6 stand rejected under 35 U.S.C. § 112, second paragraph, as it is unclear whether one passphrase generates multiple keys or a plurality of passphrases generate a corresponding plurality of keys. Official Action, p. 2. Applicants have amended Claim 5 to clarify that the personal keys are based on "the current passphrase", rather than a plurality of passphrases. Thus, the plurality of keys are based on a single passphrase. Accordingly, Applicants submit that Claims 5 and 6 are not unclear and that the rejection under Section 112 has been overcome.

The Claims Are Not Obvious

Claims 1-7, 29-35 and 57-63 stand rejected under 35 U.S.C. § 103 as obvious in light of Narasimhalu and United States Patent No. 5,495,533 to Linehan (hereinafter "Linehan") and United States Patent No. 6,023,506 to Ote (hereinafter "Ote"). Official Action, p. 2. Claims 8-10, 36-38 and 64-66 stand rejected under 35 U.S.C. § 103 as obvious in light of Linehan, Ote and United States Patent No. 5,638,448 to Nguyen (hereinafter "Nguyen"). Official Action, p. 4. Claims 11-17, 39-45 and 67-73 stand rejected under 35 U.S.C. § 103 as obvious in light of Linehan, Ote and United States Patent No. 5,734,819 to Lewis (hereinafter "Lewis"). Official Action, p. 4. Claims 18-20, 46-48 and 74-76 stand rejected under 35 U.S.C. § 103 as obvious in light of Linehan, Ote and United States Patent No. 5,805,712 to Davis (hereinafter "Davis"). Official Action, p. 6. Claims 21-28, 49-56 and 77-84 stand rejected under 35 U.S.C. § 103 as obvious in light of Linehan, Ote, Davis and Lewis. Official Action, p. 7. Applicants will address each of these rejections separately below.

Initially, Applicants note that to establish a prima facie case of obviousness, the prior art reference or references when combined must teach or suggest *all* the recitations of the claims, and there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. M.P.E.P. §2143. The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. M.P.E.P. §2143.01, citing *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990). As emphasized by the Court of Appeals for the Federal Circuit, to support combining references, evidence of a suggestion, teaching, or motivation to combine must be **clear and particular**, and this requirement for clear and particular evidence is not met by broad and conclusory statements about the teachings of references. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). In an even more recent decision, the Court of Appeals for the Federal Circuit has stated that, to support combining or modifying references, there must be **particular** evidence from the prior art as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000).

Claims 1-7, 29-35 and 57-63

Claims 1-7, 29-35 and 57-63 include independent Claims 1, 29 and 57. Each of these claims recites that a personal key is generated based on a passphrase and that the personal key is used to encrypt a file encryption key. The file encryption key is used to encrypt the file, not the personal key.

In rejecting Claims 1-7, 29-35 and 57-63 the Official Action acknowledges that Linehan does not disclose that the personal key is generated using a passphrase. Official Action p. 3. As such, Linehan does not appear to provide for combined authentication of the user and decryption of the file as the users are authenticated separately from the generation of the personal key. In particular, the passwords of Linehan do not appear to be used for key generation, but only authentication. See Linehan, col. 2, line 61 to col. 3, line 37. Furthermore, the keys in Linehan appear to be managed at the system level rather than at the client level. See Linehan, col. 7, lines 30-33. Thus, Linehan states that the control key is "known only to the Personal Key Server." Linehan, col. 9, lines 31-34.

The Official Action relies on Ote as providing the teachings that are missing from Linehan. Official Action, p. 3. Ote fails to provide the teachings missing from Linehan, namely that the key used to encrypt the key that is used to encrypt the file is itself encrypted with a key that is generated based on a passphrase. Thus, even if combined, Linehan and Ote would not result in the recitations of Claims 1, 29 and 57, which recite generating "a personal key based on the obtained passphrase" and using the personal key to encrypt, not the file, but the file encryption key.

With regard to the motivation to combine the references in the manner recited in the claims, the Official Action asserts that Ote and Linehan would be combined to result in the recitations of the claims because "a pass phrase is easy to remember and allows the user to avoid management of encryption keys." Official Action, p. 3. However, Applicants submit that such a motivation is not present in the cited references. In particular, Linehan is even simpler for the user because the keys are managed at the system level by the key server and, thus, the user does not even need to remember a pass phrase for encryption purposes, only for authentication. Furthermore, Linehan expressly states that the advantages of the systems described in Linehan include "[f]ile encryption keys are automatically managed" and "[n]o additional effort is required on the part of users." Linehan, col. 10, lines 46-48. Linehan further goes on to state that a further advantage is that "[u]sers cannot forget or lose file encryption keys. Hence there is no risk of inadvertent loss of access to data files." Linehan, col. 10. lines 66-67. Thus, Applicants submit that the motivation to modify Linehan set forth in the Official Action is not present as the identified needs solved by Ote are not present in the system of Linehan as they have already been solved by the system of Linehan.

In light of the above discussion, Applicants submit that Claims 1, 29 and 57 are patentable over Linehan and Ote. Applicants submit that the dependent claims are patentable at least as depending from a patentable base claim. Applicants also submit that certain of the dependent claims are separately patentable over the cited references. For example, with respect to Claims 5, 33 and 61, Applicants submit that it is not inherent that a single passphrase will be used to generate multiple personal keys that are used to encrypt the file encryption keys as recited in Claims 5, 33 and 61. Applicants also submit that such a use of a passphrase is not described in the cited portions of either Ote or Linehan. In fact, Ote appears to contemplate generating the same key for all files in a folder. See Ote, col. 5, lines 9-32. Accordingly, Applicants submit that Claims 5, 33 and 61 are separately patentable over the cited references for at least these additional reasons.

Claims 8-10, 36-38 and 64-66

Claims 8-10, 36-38 and 64-66 each recite specific techniques for generating the personal key used to encrypt the file encryption key. In particular, these claims recite that the personal key is generated by hashing the user identification, the passphrase and the file identification to provide the personal key. Applicants submit that these claims are patentable as depending from a patentable base claim. Applicants also submit that these claims are separately patentable over the cited references.

In particular, Applicants submit that the cited portion of Nguyen, col. 4, lines 12-16, does not disclose or suggest the use of user identification, passphrase **and** file identification to generate a personal key as recited in Claims 8-10, 36-38 and 64-66. Merely disclosing the generation of a key using user identification and a password as discussed in Nguyen does not suggest incorporating file identification in the hash as recited in the claims. Such is especially true in the present case because Nguyen does not relate to file encryption, but relates to network communications. See Nguyen, Title. As such, Applicants further submit that, in addition to Nguyen not providing the teachings that are missing from Ote and Linehan, there is no proper motivation to combine the secure network communications system of Nguyen with the file encryption systems of Linehan or Ote.

In light of the above discussion, Applicants submit that Claims 8-10, 36-38 and 64-66 are separately patentable over the cited references for at least these additional reasons.

Claims 11-17, 39-45 and 67-73

Claims 11-17, 39-45 and 67-73 recite various uses of an integrity key and message authentication code and that the integrity key is encrypted with the personal key. Additional dependent claims also recite that a verification value is generated by hashing the integrity key and the file encryption key. Applicants submit that these claims are patentable as depending from a patentable base claim, but also submit that these claims are separately patentable over the cited references.

For example, Claims 11, 39 and 67 recite that the integrity key is encrypted with the personal key. None of the cited references disclose or suggest encrypting an integrity key used to generate the message authentication code with a personal key. In fact, the cited portion of Lewis states only that the key used to generate the message authentication code is kept secret. Lewis, col. 2, lines 20-21. It is not inherent that the key be encrypted to keep it safe. In fact, the cited portion of Linehan, col. 8, lines 62-65, does not disclose including a key for generating the message authentication code in the file header, thus, there would be no need to encrypt the key as it would not be sent with the file header. Furthermore, Lewis relates to storing security information in a non-volatile memory and preventing operation of a computer if tampering is detected, whereas Linehan and Ote relate to file encryption. See Lewis, col. 1, lines 7-15. As such, Applicants further submit that, in addition to Lewis not providing the teachings that are missing from Ote and Linehan, there is no proper motivation to combine the secure network communications system of Lewis with the file encryption systems of Linehan or Ote.

Likewise, Claims 14, 42 and 70 recite that the integrity key is hashed with the file encryption key to provide a verification value. None of the cited portions of Linehan, Ote or Lewis disclose the generation of a verification value as recited in these claims.

In light of the above discussion, Applicants submit that Claims 11-17, 39-45 and 67-73 are separately patentable over the cited references for at least these additional reasons.

Claims 18-20, 46-48 and 74-76

Claims 18-20, 46-48 and 74-76 relate to shared access to the encrypted file by public key cryptography and incorporating into the header a version of the file encryption key that is encrypted with the public key of users authorized to access the file. Applicants submit that these claims are patentable as depending from a patentable base claim. Applicants also submit that these claims are separately patentable over the cited references.

The Official Action cites to Davis, col. 2, lines 3-10 as providing the teachings missing from Linehan and Ote regarding public key cryptography. Official Action, p. 6. However, the cited portion of Davis does not disclose using a public key to encrypt a file encryption key as recited in Claims 18-20, 46-48 and 74-76. Applicants are not claiming to have invented public key cryptography, but a specific use of public key cryptography. That specific use is not disclosed or suggested by the cited portions of Linehan, Ote or Davis. In particular, the use of public key cryptography to encrypt the file encryption key so as to incorporate file access control into the header of the file as recited in these claims is not suggested by the cited portions of Linehan, Ote and/or Davis.

The Official Action asserts that it would be obvious to combine Linehan and Ote with the public key teachings of Davis "because the public key system alleviates key management associated with symmetric key cryptography." Official Action, p. 7. However, there is no need to modify Linehan because Linehan already incorporates a system for shared file access that does not use public key cryptography by incorporating the access control list in the file header. See Linehan, FIG. 8.

In light of the above discussion, Applicants submit that Claims 18-20, 46-48 and 74-76 are separately patentable over the cited references for at least these additional reasons.

Claims 21-28, 49-56 and 77-84

Claims 21-28, 49-56 and 77-84 include recitations analogous to those of Claims 11-20, 39-48 and 67-76. Applicants submit that these claims are patentable as depending from a patentable base claim. Applicants also submit that these claims are separately patentable over the cited references for reasons analogous to those discussed above with reference to Claims 11-20, 39-48 and 67-76.

Conclusion

In light of the above discussion, Applicants submit that the present application is in condition for allowance, which action is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,

Timothy J. O'Sullivan
Registration No. 35,632

USPTO Customer No. 46589

Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401